REMARKS/ARGUMENTS

The present amendment is submitted in accordance with the Revised Amendment Format.

The Examiner has required new corrected drawings in compliance with 37 C.F.R. 1.121(d).

The Examiner has objected to the specification because of informalities on page 18 at line 7.

The Examiner has objected to claims 31-43 because of informalities.

The Examiner has rejected claims 1-4, 6, 9-14, 16-19, 22-24, 31, 35, 36, 40, 41 and 43 of this Application under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 6,292,782 to Weideman.

The Examiner has rejected claims 7, 8, 15, 32-34, 38 and 39 of this Application under 35 U.S.C. § 103(a) as being unpatentable over Weideman in view of U.S. Patent No. 6,691,089 to Su et al. (herein, "Su").

The Examiner has rejected claims 20, 21 and 37 of this Application under 35 U.S.C. § 103(a) as being unpatentable over Weideman in view of U.S. Patent No. 6,049,785 to Gifford.

The Examiner has rejected claims 25-27 and 42 of this Application under 35 U.S.C. § 103(a) as being unpatentable over Weideman in view of U.S. Patent No. 5,774,525 to Kanevsky et al. (herein, "Kanevsky").

The Examiner has rejected claims 28-30 of this Application under 35 U.S.C. § 103(a) as being unpatentable over Weideman in view of U.S. Patent No. 6,700,953 to Maurer et al. (herein, "Mauer").

Independent claims 1, 9 and 31 have been amended.

Dependent claim 3 has been amended to correct a typographical error.

Dependent claims 38, 40 and 42 have been amended to more clearly define what Applicant regards as alternative embodiments of the invention.

Claim 43 has been canceled.

All amendments are fully supported by the specification and no new matter has been added.

Interview Summary

On December 8, 2004, Applicant's Attorney conducted an interview with the Examiner. Applicants thank the Examiner for the interview. During the interview, the allowability of the claims was discussed. As set forth below, Applicants pointed out to the Examiner that Weideman does not disclose the invention as described by the claims (amended or unamended). The central issue discussed was whether or not disclosure of "recognition" on the client in Weideman also discloses "security authorization" as found in, for example, independent claim 1. In particular, Applicant's contended that Weideman does not disclose "security authorization" on *both* the client and server, but rather recognition alone. Examiner contended that recognition by itself is "security authorization." Examiner and Applicant's Attorney reached an impasse on the issue.

Rejection under 35 U.S.C. § 102(b) based on Weideman

A. Applicable Law:

"A claim is anticipated under 35 U.S.C. § 102(b) only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *Verdegaal Bros. V. Union Oil Co. of* California, 814 F.2d 628, 631 (Fed. Cir. 1987), MPEP 2131.01. The Federal Circuit has repeatedly emphasized that anticipation is established only if (1) all the elements of an invention, as stated in the patent claim, (2) are identically set forth, (3) in a single prior art reference. *In re Schreiber*, 128 F.3d 1473, 1477 (Fed. Cir. 1997) ("To anticipate a claim, a prior art reference must disclose every limitation of the claimed invention, either expressly or inherently."); *In re Paulsen*, 30 F.3d 1475,1478-79 (Fed. Cir. 1994) ("A rejection for anticipation under section 102 requires that each and every limitation of the claimed invention be disclosed in a single prior art reference."); *Gechter v. Davidson*, 116 F.3d 1454, 1457 (Fed. Cir. 1997) ("Under 35 U.S.C. 102(b), every limitation of a claim must identically appear in a single prior art reference for it to anticipate the claim").

Importantly, the presence of each claim limitation in the disclosure of a reference must be clear. For example, as stated in *Datascope Corp. v. SMEC, Inc.*, "Anticipation cannot be predicated on teachings in a reference that are vague or based on conjecture." *Datascope Corp. v. SMEC, Inc.*, 776 F.2d 320 (Fed. Cir. 1985). This concept has been reiterated by the Board of Patent Appeals. For example, in *Ex parte Standish*, the Board stated, "anticipation of a claimed product cannot be predicated on mere conjecture as to the characteristics of a prior art product." *Ex parte Standish*, 10 USPQ2d 1454, 1457 (Bd. Pat. App. & Int'f 1989).

B. Application of the Law and Reference to the Claims At-Issue:

The Examiner's rejection of independent claims 1, 9 and 31 of this Application under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent No. 6,292,782 to Weideman are not supported by the Weideman's disclosure. Applicants have amended claims 1, 9 and 31 to more clearly distinguish recognition alone from security authorization (which may include recognition but also includes additional steps). Claims 1, 9 and 31 are allowable because Weideman does not clearly disclose each and every element recited in these claims either expressly or inherently. For example, amended claim 1 recites:

> a client system receiving first biometric data and having a first level security authorization procedure, wherein the first level security authorization denies access to the client system if the first biometric data does not correspond to an authorized user; and
>
> a server system receiving second biometric data and having a second level security authorization procedure;
>
> wherein the first level security authorization procedure and the second level security authorization procedure comprise distinct biometric algorithms.

1. Weideman does not disclose first and second biometric data

Weideman does not disclose first and second biometric data for first and second security authorizations. During the above-mentioned interview, the Examiner stated that Weideman's disclosure of speech data and encrypted speech data could be interpreted as anticipating "first biometric data" and "second biometric data" because the encrypted speech data is "second biometric data." However, while Examiners are entitled to give claim language in a pending patent application a broad interpretation, such interpretations must be "consistent

with the specification" of such application. The Examiner's contention that speech data and an encrypted version of the same speech data is the same as first and second biometric data as found in claim 1 is altogether inconsistent with the specification of the present application. While the specification discloses many embodiments of the first and second biometric data, including different types of biometric data, such as speech and fingerprints, or different portions of biometric data, such as a first and second portion of a single speech pattern, the specification does not disclose anything to suggest that the second biometric data could be an encrypted version of the first biometric data.

Indeed, such a definition is inconsistent with the specification because the specification discloses using different biometric data, or different portions of the same data, for the client and server security algorithms. If an encrypted version of the first biometric data were used as the second biometric data on the server, the second biometric data would have to be decoded (i.e., unencrypted) before the second security algorithm could operate. Thus, both the client and the server would be using the same biometric data for authorization.

2. Weideman does not disclose distinct biometric algorithms

As illustrated above, claim 1 includes the limitation that "the first level security authorization procedure and the second level security authorization procedure comprise distinct biometric algorithms." However, Weideman does not disclose distinct biometric algorithms on the client and server. Rather, as set forth below, Weideman discloses a speech recognition algorithm on a client and the same speech recognition algorithm on the server. Assuming arguendo that the speech recognition algorithms were performing security functions (which they don't) and were the same as the first and second "security authorization procedures" (which they are not), Weideman's disclosure would still fail to anticipate claim 1 because Weideman discloses that the speech recognition algorithms are the same on both the client and server. In particular, the only recognition algorithm disclosed in Weideman is described in Fig. 3. A reference cannot anticipate distinct biometric algorithms on the client and server where only one algorithm is disclosed, as is the case here.

Furthermore, if the Examiner is taking the position that Weideman discloses "a client and server using distinct algorithms" on the grounds that Weideman's client performs only

recognition whereas Weideman's server performs both recognition and verification, then the Examiner must concede that recognition is fundamentally different from verification. More specifically, and as set forth in more detail below, if recognition and verification are different (and thereby distinct algorithms), then recognition cannot be a "security authorization."

3. Weideman does not disclose "security authorization" on the client

The Examiner has taken the position that Weideman discloses "security authorization" on the client because Weideman discloses "recognition" on the client. However, this is improper conjecture. Weideman does not disclose any security authorization procedure being conducted on the client. Indeed, the disclosure in Weideman is inconsistent with such a position.

Wiedeman discloses a partitioned system for performing speech recognition on networked computer systems (e.g., a client and server). As stated in the Summary of the Invention,

> "The user speaks an identifier into a microphone connected to the client unit and the spoken data comprising the identifier is converted into speech feature data. This conversion is carried out by a locally resident software application or may be done by an application or plug-in applet that has been downloaded from the server unit in response to the requested transaction.
>
> The speech feature data is transmitted over a computer communication link from the client unit to the server unit for further processing. ... A speech recognition engine located at the server unit uses the speech feature data to identify and confirm the spoken identifier entered by the user. The speech feature data is then further processed by the speech verification engine to confirm that the user who entered the spoken identifier is in fact the user associated with the spoken identifier and is authorized to perform the requested transaction."

(Weideman, Summary of the Invention, col. 1, line 67, col. 2, lines 1-19.)

This portion of Weideman's disclosure illustrates that the client transforms the incoming spoken data into "speech feature data." The "speech feature data" is then transmitted to the server, wherein two distinct processes occur. First, the speech feature data is processed by a "recognition engine" to "identify and confirm the spoken identifier." Second, the speech

feature data is processed by a "verification engine," which is the ONLY engine to "authorize" a user.

Fig. 3 of Weideman further illustrates the partitioned nature of the system disclosed in this prior art. With regard to Fig. 3, Weideman discloses the following:

> "Referring now to FIG. 3, a block diagram is shown of an embodiment of the voice recognition and verification algorithms 48 and 50. The functional blocks set forth in the upper portion of the block diagram comprise those steps which are performed by the speech feature application 20 located on the client unit."

(Weideman, col. 4, lines 32-37, Emphasis Added.)

Weideman goes on as follows:

> "As can be seen then, the upper portion of FIG. 3 represents the first tier of the multistage data reduction process which significantly reduces the amount of data to be analyzed and transferred..."

(Weideman, col. 5, lines 9-12.)

With regard to the server, Weideman states:

> "the middle portion of FIG. 3 represents a second tier of the data reduction process, and as will be described, comprises transformation routines 49a and 49b occurring at the voice verification and recognition engines 22 of the server unit 12 (FIG. 1)."

(Weideman, col. 5, lines 15-19, Emphasis Added.)

Thus, Weideman discloses a partitioned system wherein a client includes a "speech feature application" (see Fig. 1, element 20 and Fig. 3, blocks 60 and 62-65) that "enables the conversion of speech data to speech feature data for transmission over the computer network..." (Weideman, Col. 3, lines 6-8) The client system in Weideman does not perform verification or any other form of security authorization.

However, the Examiner has stated that "a client system receiving first biometric data and having first level security authorization procedure" as found in claim 1 is anticipated by

the disclosure at col. 3, lines 51-59 and Fig. 2a, step 31. The relevant portions of col. 3 state as follows:

> "In the embodiment of FIG. 2a, the transformed speech data may be initially recognized at optional step 31 to confirm that the identifier can be correctly identified by the speech recognizer prior to transmission of the data. This step would use the speech recognition algorithm as will be described more fully in a moment."

(Weideman, col. 3, lines 51-59, Emphasis Added.)

This section of Weideman's disclosure does not disclose "a client system receiving first biometric data and having first level security authorization procedure" because the above cited portion of Weideman does not disclose any form of authorization. Recognition alone is not a "security authorization procedure." This fact is most clearly illustrated by referring to the portion of Weideman that describes the recognition algorithm. From the emphasized portion of the above exert, the recognition algorithm used by the client in Weideman is the same as the recognition algorithm on the server, which is described as follows:

> "To effect speaker independent voice recognition, the tertiary features are first supplied to the voice recognition linear transformation routine 49a. ... The output of the transformation routine 49a is then applied to a voice recognition statistical decision routine 66a for comparison with a voice recognition class of reference data 54. The output of the decision routine 66a is a yes/no decision identifying whether the digit is recognized and, if so, which digit was spoken."

(Weideman, col. 5, lines 20-30, Emphasis Added.)

Thus, Weideman discloses recognition on the client, but there is no form of "authorization" on the client. This distinction is clarified by the portion of Weideman's disclosure that does describe "authorization;" namely, the "verification engine" on the server.

> "To effect voice verification, the tertiary features are also supplied to a linear transformation routine 49b ...
> Verifier routine 66b generates one of three different outputs: ACCEPT, REJECT and TEST. An ACCEPT output may authorize the user to from the transaction database.

(Weideman, col. 5, lines 53-54 and col. 6, lines 1-3, Emphasis Added.)

Thus, by comparing the outputs of the recognizer and verifier engines disclosed in Weideman, it is clear that ONLY the verification engine provides outputs that support authorization. The purpose of the recognition engine in Weideman is ONLY to determine whether recognition is possible using the spoken inputs. If the spoken input is not properly recognized (i.e., if a "no" result is returned from the recognition engine), then "the user is prompted to reenter the phrase or identifier." (Weideman, col. 3, line 59) The first element of claim 1 reads as follows:

> a client system receiving first biometric data and having a first level security authorization procedure, wherein the first level security authorization denies access to the client system if the first biometric data does not correspond to an authorized user; and

There is absolutely no disclosure in Weideman that a recognition engine on the client performs any form of "authorization" or that such a recognition engine "denies access to the client system if the first biometric data does not correspond to an authorized user." Rather, authorization and access control exist solely on the server in Weideman. Because the recognition engine disclosed in Weideman does not support "authorization" and does not control access, such a recognition engine does not, and cannot, anticipate "security authorization procedure" as found in claim 1. Therefore, Weideman does not include all the elements of claim 1 and cannot anticipate claim 1 under 35 U.S.C. § 102(b).

Claims 2-8 are dependent claims that include all the limitations of claim 1 and include additional limitations. Therefore, these claims are allowable for at least the same or similar reasons.

Claim 9 is allowable for similar reasons. For example, amended claim 9 recites:

> receiving a first level security authorization signal on the server system from a client system, wherein the first level security authorization signal indicates that the client system has authorized a user of the client;
>
> receiving biometric data on the server system from the client system;

executing a second level security authorization, the second level security authorization including analyzing the biometric data using a first biometric algorithm on the server system; and

generating a second level security authorization signal on the server system when the first biometric algorithm indicates that the biometric data corresponds to one of a plurality of users authorized to access the server system.

Among other things, Weideman does not disclose "receiving a first level security authorization signal from a client" and "executing a second level security authorization" on a server. As mentioned above, Weideman discloses a client that performs recognition alone, which is not a security authorization and does not produce a security authorization signal. Because the client disclosed in Weideman does not include any form of security authorization and does not include a security authorization signal being received by the server, Weideman does not include all the elements of claim 9. Consequently, Weideman cannot anticipate claim 9 under 35 U.S.C. § 102(b).

Claims 10-30 are dependent claims that include all the limitations of claim 9 and include additional limitations. Therefore, these claims are allowable for at least the same or similar reasons.

Claim 31 is allowable for similar reasons. For example, amended claim 31 recites:

receiving biometric data in the client system;

analyzing a first portion of the biometric data using a first biometric algorithm on the client system, wherein the first biometric algorithm denies access to the client system if the first portion of biometric data does not correspond to an authorized user;

generating a first level security authorization signal on the client system when the first biometric algorithm indicates that the first portion of the biometric data corresponds to an authorized user;

transmitting the first level security authorization signal and second portion of the biometric data to a server system, the second portion of biometric data being analyzed by a second biometric algorithm on the server; and

accessing resources on the server system through the client system when the second biometric algorithm provides a second level security authorization.

As mentioned above, Weideman does not disclose a biometric algorithm that denies access to the client system if the first portion of biometric data does not correspond to an authorized user. Furthermore, Weideman does not disclose generating a "security authorization signal" on a client "when the first biometric algorithm indicates that the first portion of the biometric data corresponds to an authorized user." Moreover, Weideman does not disclose analyzing a first portion of biometric data on a client using a first biometric algorithm and transmitting a second portion of biometric data and a security authorization signal to the server. Thus, Weideman does not include all the elements of claim 31, and cannot anticipate claim 31 under 35 U.S.C. § 102(b).

Claims 32-42 are dependent claims that include all the limitations of claim 31 and include additional limitations. Therefore, these claims are allowable for at least the same or similar reasons.

CONCLUSION

In view of the foregoing, Applicants believe all claims now pending in this Application are in condition for allowance. The issuance of a formal Notice of Allowance at an early date is respectfully requested.

If the Examiner believes a telephone conference would expedite prosecution of this application, please telephone the undersigned at 408-244-6319.

Respectfully submitted,

Chad R. Walsh
Reg. No. 43,235

FOUNTAINHEAD LAW GROUP
6172 Bollinger Road #174
San Jose, CA. 95129

Tel: 408-244-6319
CRW